

Volume 2, Issue 8
July 2020

ARMY COMMUNICATOR

Passing the Guidon

Plus:

- **Virtual Conferencing**
- **Satellite Tech**
- **Cyber Warfare**



Contents

3.
Command Team
4.
Passing the baton
6.
Emerging satellite technologies
10.
Bridging the joint communications gap at the technician level
12.
Leveraging Microsoft Teams for virtual conferencing
19.
Early insights into electronic and cyber warfare at the battalion level

The Army Communicator is published as a command information e-publication for the men and women of the United States Army Signal Corps under the provisions of AR 360-1.

Opinions expressed herein do not necessarily reflect the views of Office, Chief of Signal, the US Army or the Department of Defense.

Submit articles, photos, graphics, videos, story ideas, and nominations for “Signal Spotlight” to the editor [here](#). For additional information, please call (706) 791-7384.

Follow the Signal Regiment on Facebook [here](#).

Follow the Signal School Commandant on Twitter [here](#).

COL John T. Batson
Acting Signal School Commandant

CSM Darien D. Lawshea
Signal Corps Command Sergeant Major

CW5 Garth R. Hahn
Signal Corps Chief Warrant Officer

Nicholas M. Spinelli
Editor-in-Chief

On the Cover

Maj. Gen. Neil S. Hersey, Fort Gordon Commanding General, (center) passes the guidon from Brig. Gen. Christopher L. Eubank (right) to Col. John T. Batson.

Photo by Nick Spinelli



Chief of Signal Regimental Team

Welcome to the July edition of the Army Communicator! Command Sergeant Major (CSM) Lawshea and I are excited to be joining the team with this issue.

Experience has taught us that although assumption and relinquishment of responsibility are clearly delineated with specific dates, the impact that leadership teams have on Soldiers, the mission, and the surrounding community is enduring. Each new leadership team takes the proverbial baton for their leg of the relay and attempts to advance the organization to a place where future leadership teams, similar to us, have a head-start due to standing on the shoulders of giants. We are excited to take the baton and will work tirelessly to ensure that when the time comes to pass the baton to the next team, they too will be set-up for success. CSM Lawshea, CW5 Hahn, and I are all honored to be leading this leg of the relay, and we promise to carry the baton to the best of our abilities.

Last month, the Army Communi-

cator took a deep dive into the history of the U.S. Army Signal Corps. The historical focus of that edition of the Communicator perfectly aligns with the Signal Corps celebrating its 160th anniversary this year. Although the Signal Corps, and its Soldiers, evolved over time, from the innovative and resilient BG Albert J. Myers, to the incredibly technical, proficient, and multi-functional Signal Soldiers of today, it continues to impact missions and give command on battlefields and global span. The Signal Corps' mission of "getting the message through" in denied, degraded, and disrupted operational environments is a no-fail mission and we are eager and excited to take the mission! In this issue we will be shifting from looking back to looking ahead at emerging ideas and technologies that offer exciting potential for the future of Signal operations.

If you have ideas for what you would like to see in upcoming issues of the Army Communicator, or if you want to submit an article yourself, please feel free to contact us. Enjoy this issue, and until next time...

Pro Patria Vigilans!



COL John T. Batson
Acting Signal School Commandant



CSM Darien D. Lawshea
Regimental CSM



CW5 Garth R. Hahn
Regimental CWO

New leadership takes charge of Signal

Nick Spinelli
Office Chief of Signal

Change came to the US Army Signal School last month with the arrival of the new leadership team, Col. John T. Batson and Command Sgt. Maj. Darien D. Lawshea.

The two assumed responsibility of both the schoolhouse and the Signal Regiment in ceremonies held June 5 for command sergeant major and June 8 for the commander.

“Thank you for the confidence you all have placed in me as I assume these responsibilities as acting commandant during this period of transition,” Batson said. “The Signal School is in the business of training and educating multi-domain, multi-disciplined Signal Officers and Soldiers. I look forward to continuing that standard of excellence.”

Command Sgt. Maj. Lawshea expressed similar gratitude at his ceremony a few days earlier.

“Thank you for giving me

this opportunity and for also trusting me to carry on the message of our regiment,” he said. “I am committed to ensuring our continued success as we forge into a new era of changing requirements to the Force.”

The outgoing commandant, Brig. Gen. Christopher L. Eubank, oversaw many changes and additions during his tenure as Chief of Signal, such as the Enlisted MOS convergence project, the launch of the Expeditionary Signal Brigade-Enhanced, and countless others, including the transition of this publication to a digital product.



From left: Col. John T. Batson, Maj. Gen. Neil S. Hersey, and Brig. Gen. Christopher L. Eubank
Photo by Nick Spinelli



Col. Edward W. Kendall
Photo by Nick Spinelli

“Under Brig. Gen. Eubank’s leadership, the Signal School embraced and led change, shaped the Signal Corps of the future, and achieved great outcomes and great accomplishments,” Maj. Gen. Neil S. Hersey, Fort Gordon Commanding General, said.

During his remarks, Eubank refused to take the credit for the past two years of Signal success, instead expressing gratitude to the entire team for their accomplishments.

“When I wrote [these remarks] I didn’t realize how long it was going to take based on how many people I wanted to thank,” he said. “Thank you to all the Soldier, civilians, and contractors who make up the Signal School, and truly are the heroes of this organization. Thank you for continuing to push the ideas, innovation, and regiment into the future.”

The Signal School wasn’t the only organization see a change in leadership, though. As Col. Batson assumed the role of Acting Signal School Commandant, his previous position of 15th Signal Brigade Commander was filled by Col. Edward W. Kendall.

“Thank you for the trust and confidence you have in me, and for providing me the opportunity to command. It truly is a privilege and an honor to join this great team,” Kendall said.

Due to COVID-19 pandemic, all three ceremonies were conducted virtually. Attendance was minimal, limited only to participants and immediately family. They were recorded and shared via social networking sites for wider audiences. Maj. Gen. Hersey acknowledged the scaled down nature of the ceremonies, which would traditionally be held on a parade field with much larger audiences.

“Thank you to our viewers on social media as we use technology to ensure that everyone has a chance to view [these historic ceremonies] in a restrained COVID-19 environment.” Hersey said. “You have all risen to the occasion of combating a hidden enemy of COVID-19 by maintaining social distancing and by taking the necessary precautions to keep yourselves and others safe.”

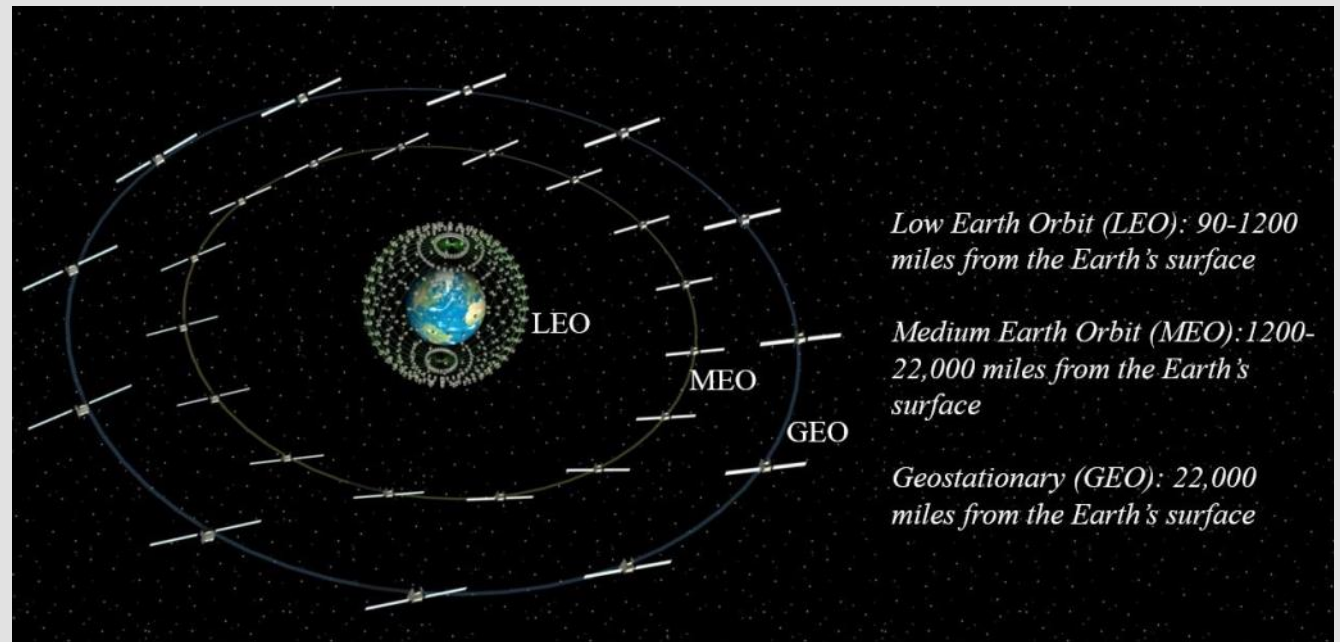


Command Sgt. Maj. Darien D. Lawshea
Photo by Nick Spinelli

Emerging LEO, MEO, GEO satellite technologies – more bandwidth, less latency

John Anglin, Project Manager Tactical Network (PM TN) Technical Management Division Chief; Seth Spoenlein, Senior Scientific Technical Manager for Integrated Networks at Army Futures Command (AFC) Combat Capabilities Development Command (CCDC) C5ISR Center; and Amy Walker, PM TN/PEO C3T public affairs

The Army is working across its acquisition, modernization, and research and development communities, joint partners and industry to experiment with evolving Low Earth Orbit (LEO) mega-constellations, and Medium Earth Orbit (MEO) and Geostationary high throughput satellite technologies to better understand how they could fuel the network of the future. The Program Executive Office for Command, Control, Communications-Tactical (PEO C3T); Network-Cross Functional Team (N-CFT); and the Combat Capabilities Development Command (CCDC) C5ISR Center are working closely with



Graphic provided by PEO C3T

industry to build a focused roadmap and test plan to allow emerging satellite communications capability to be run through its paces in future training and capability exercises over the next couple of years. These events will inform Army decisions on how innovative technologies could best integrate into the greater network.




The Army's current satellite capability provides at-the-halt and on-the-move beyond-line-of-sight network communications to Soldiers dispersed over large regions in remote and challenging terrain. The service leverages a mix of commercial and military satellites in the Earth's geosynchronous orbit. The Army is reevaluating its satellite communications architecture to incorporate both military and commercial solutions across GEO, MEO, and LEO constellations. This diversity would allow for the optimization of the best solution set, while making the network more robust.

So what's the physical difference between LEO, MEO and GEO satellites? LEO satellites orbit between 90 and 1200 miles from the Earth; MEO satellites orbit from 1200 to 22,000 miles from the Earth's surface; and large Geosyn-

chronous Earth Orbit (GEO) satellites orbit furthest away at 22,000 miles. MEO and LEO constellations require more satellites than GEO to achieve required coverage. MEO constellations will typically require tens of satellites where LEO requires hundreds and even thousands of satellites orbiting the Earth. GEO satellites appear stationary from a point on the Earth's surface, where LEO and MEO move across the sky and require additional tracking and handover capability between satellites.

Each solution has its own strengths and weaknesses, and there will not be a final one-size-fits-all solution -- different threats may require different solutions. Instead, the



ORBIT TYPES		ALTITUDE (MILES)
	Low Earth Orbit	Up to approximately 1,200
	Medium Earth Orbit	Approximately 1,200 to 22,000
	Geosynchronous Earth Orbit	Approximately 22,000

Graphic provided by PEO C3T

Army will capitalize on the strengths of all of these evolving capabilities to provide commanders and signal officers with multiple network communication capabilities and signal path options to optimally support their missions.

LEO and MEO satellite communication capabilities are expected to provide huge increases in network bandwidth, while significantly reducing latency, which are both must-haves for many of the Army's network modernization efforts. When compared to current GEO solutions, the anticipated deployment of mega-constellations operating in LEO could provide a 100 times increase in bandwidth and a 10 times reduction in latency, while providing network communications services to a larger density of users. MEO bandwidth increases will be slightly less, but significantly more than current GEO capability provides. Bottom line: these improvements will enable more data to be sent at faster rates to a larger number of users.

The anticipated proliferation of LEO and MEO satellite capabilities by commercial industry provides the potential to significantly increase the communications capacity for a large density of Soldiers across the Army. It would deliver expeditionary, mobile, beyond-line-of-sight communications with increased bandwidth and low latency to better enable the Army's mission command systems.

High Throughput Systems in GEO, LEO and MEO solutions are also expected to reduce stress on overburdened military GEO satellite capability and provide more connection options for increased network resiliency. Since LEO satellite constellations will contain numerous small satellites at a much lower altitude, there is a natural physical resiliency that comes with having so many satellites. The signals don't have to travel as far to get to the satellite, so the latency is significantly reduced. The reduced latency will significantly improve the performance of the network, especially for real-time applications.

Among many potential implementations, these LEO and MEO capability benefits are expected to enhance the Army's ability to implement artificial intelligence data aggregation and leverage edge cloud services that enable Soldiers to gain access to data and software previously available only at large data centers. If inter-satellite links are successfully implemented, these solutions could also enable the Army to put more complex network functions and mission support capabilities in safe sanctuaries, pulling complexity out of tactical echelons

and putting it in locations where it can be effectively maintained with more resources in a less contested environment.

Of significant importance, the Army plans to use future LEO and MEO solutions to support Joint All Domain Command and Control, or JADC2 -- a major effort that will leverage capabilities across all domains and mission partners to achieve battlefield advantage. In support of JADC2, the Army plans to deliver network transport and data management solutions to enable the flow of critical situational awareness and sensor data, to connect sensors (such as aircraft, radar and Soldier-wearable devices), to shooter, (the weapons systems that attack targets), all the way down to the dismounted Soldier. New LEO and MEO systems could deliver the needed improvements in network latency, capacity and resiliency to enable data convergence of mission command, fires, sustainment and intelligence data, and to

push all of that aggregated data from the Army's common operating environment to the JADC2 network.

As part of its network modernization strategy, the Army is delivering phased network capability enhancements every two years, beginning with Capability Set 21 in fiscal year 2021. The Army will build on lessons learned from the development and fielding of each capability set, including work being done with new and evolving satellite capabilities.

The Army plans to leverage a mix of multiple military and commercial satellite constellations to support its overall satellite network communications architecture. The service will continue to leverage GEO satellites currently in use, and add capability to leverage emerging constellations. These include commercial

LEO and MEO mega-constellations; commercial high throughput satellites; and the extremely resilient Protected Tactical Satellite communications (PTS) military GEO satellite system in development by the Air Force.

This kind of diversity through multiple signal paths provides desirable network redundancy, however, it also increases overall network complexity. Research and development investments, as well as engagements with industry, are underway to address these and other challenges. Considerations could possibly include the exploration of new processes and business methods, such as following a managed service model.

While the Army will leverage spacecraft developed by other



*In January 2020, the PEO C3T, N-CFT, and the CCDC C5ISR Team concluded the initial phases of Medium Earth Orbit satellite testing with prototype ground satellite terminals, at the C5ISR Center Joint Satellite Communications Engineering Center, Aberdeen Proving Ground, Maryland.
Photo by Amy Walker*

government agencies and commercial providers, and not build its own satellite communications space network, challenges exist with the integration of the satellite communications components into the terrestrial network, as well as providing the ground antennas that could support ruggedized on-the-move network capabilities. Just how to integrate some of these solutions with soldiers and onto platforms is being explored.

The Army's multi-



In January 2020, the PEO C3T, N-CFT, and the CCDC C5ISR Team concluded the initial phases of Medium Earth Orbit satellite testing with prototype ground satellite terminals. Photo by Amy Walker

constellation strategy will require different ground terminals and eventually integrated multi-functional ground terminals. Today, each GEO, MEO, and LEO solution requires its own dedicated antenna, which increases size, weight, and power requirements. The Army is exploring integrated terminals that support multi-orbits and frequency bands, while leveraging the anticipated significant component cost reduction that comes as a result of the commercial deployments. Initially, for Capability Set 23, the Army envisions using a single frequency-band ground terminal supporting one specific constellation. Integrated terminals capable of supporting multiple bands and constellations will eventually be developed for future capability sets.

The Army's initial experimentation is focused on testing commercial services, while evaluating various ground antenna solutions. In January 2020, the PEO C3T, N-CFT, and the CCDC team concluded the initial phases of MEO testing, at the C5ISR Center Joint Satellite Communications Engineering Center, Aberdeen Proving Ground, Maryland. The experimentation characterized current emerging MEO capability to see how the Army's tactical network performed over the commercial MEO constellation, and it provided MEO constellation and terminal solution performance data and lessons learned to help inform capability set design decisions.

The CCDC C5ISR Center is leading and pulling together the LEO test and experimentation efforts, with PEO C3T and N-CFT monitoring these efforts as they evolve. The focus is on understanding specific LEO mega-constellation system technical operation and system requirements and analyzing ground terminal technology. CCDC C5ISR is working numerous LEO cooperative research and development agreements, known as CRADAs, with multiple companies to test their services and antennas. Experimentation timeframes will be driven by terminal availability and constellation coverage. CCDC C5ISR has also partnered with the Air Force Strategic Development Planning and Experimentation office to award experimentation contracts for emerging ground terminals operating over LEO, MEO and GEO constellations.

Winning tomorrow's wars against peer and near peer adversaries requires U.S. forces to stay ahead in the technology race. Innovations in artificial intelligence, cloud computing, and networking on-the-move will require significant enhancements in satellite communications transport, which could be realized through LEO, MEO and high throughput GEO satellite systems.

Bridging the joint communications gap at the technician level

Cpt. Trevor Smith
US Army Signal Activity-
Okinawa

The Indo-Pacific Command's theater of operations is among the most diverse in the Department of Defense. Each service is substantially represented from Hawaii to India and Antarctica up to Russia. From major joint exercises on the Korean Peninsula to freedom-of-navigation operations in the southwest Pacific, there are real-world operations and training exercises continuously being conducted throughout this theater.

Beyond line-of-sight communications are critical to command and control in this theater and the Defense Information Systems Agency (DISA) has established Large Satellite Communications Gateways (LSG) in order to meet this requirement. LSGs provide multiband, multimedia, and worldwide reach-back capabilities to the Defense Information System Network (DISN). The LSG at Buckner

Communications Site is strategically located in Okinawa, Japan, and is operated and maintained by the Army. Approximately two-thirds of the site's customers are Navy and Marine Corps with Army, Air Force, and joint missions comprising the remaining third.

There are several challenges to communicating in a joint environment including differences in terminology, technical baselines, and departmental directives. Branches use different satellite terminals that perform similar functions and use the same services as other branches. We may use the same hardware but refer to the equipment by different names and have different versions of software. For example, the Navy uses shorthand orderwire messages for operator-to-operator (OTO) communications due to low bandwidth available at sea. Services themselves will have different equipment from battalion to battalion or ship to ship due to delays in new equipment fielding or unit-specific limitations. Services also use different baselines for their equipment that are directed at different levels of their command, depending on the service and unit. An example would be between the Navy Global Communication Information Bulletin (GCIB) and DISA Circulars, where baseline information from the GCIB may conflict with satellite commu-



*LNOs from Marine 7th COMM BN learn troubleshooting procedures at Buckner.
Photo provided by Cpt. Trevor Smith*

nications guidelines from DISA. In addition to these challenges, service members oftentimes do not report to their initial assignment with the required training to perform their duties.

In order to bridge this gap an initiative was started to exchange communicators between the Buckner LSG and the units they support. Soldiers from the LSG have spent time in the field with Marines and Soldiers in order to see firsthand the challenges their customers are faced with in a



Spc. Nelson working with IT3 Jacobs from CTF-76 as part of the technician exchange at Buckner Gateway.

Photo provided by Cpt. Trevor Smith

tactical environment. The site also send Soldiers to Navy ships while they are at port and at sea. In return, the supported units send their Soldiers, Marines, Sailors, and Airmen to Buckner to learn the gateway side of the process from mission building to troubleshooting. These technicians spend time as liaison officers to their respective units during major exercises or visit to learn specific aspects of the satellite communications support process. No one wants to lose a key member of the team for an extended period of time but sending the best technicians on these exchanges will yield the most dividends.

Recently the Buckner LSG embarked a Soldier with the USS Wasp, a multi-purpose amphibious assault ship, for two months in support of Exercise Talisman Saber. The exercise is held biennially between the U.S. Military and the Australian Defense Force. The Soldier spent his time embedded with the CTF-76 N6 personnel. He was a critical link between the LSG and the ship throughout the exercise. In addition to the direct support he provided the ship's communications team, the Soldier brought priceless lessons learned back to the LSG from his experience working with the Sailors and Marines.

The challenges to communicating in a joint environment are not likely to go away anytime soon but the technician-to-technician interactions that the exchange program advances have shown to vastly decrease the "distant end" sentiment. Although the joint environment amplifies the challenges, versions of this program can still be conducted within the Army to bridge the gap between strategic and tactical communicators.



Soldiers train the 7th Marines BN communications team on the SMART-T.

Photo provided by Cpt. Trevor Smith

Leveraging Microsoft Teams for virtual conferencing

Maj. Timothy Walsh
US Army Pacific G6

On May 19 and 20, amid travel restrictions and minimum mission essential manning orders due to the COVID-19 pandemic, the United States Army Pacific (USARPAC) hosted the Indo-Pacific Landpower Conference (IPLC), a virtual event involving 90 participants including army chiefs of staff and consul generals from 23 nations, broadcast live to a wider audience of subordinate leaders. The intent of senior USARPAC leaders was to meet strategic objectives in the information environment by replacing the annual LANPAC symposium, which the Association of the United States Army (AUSA) canceled due to the pandemic.

The USARPAC G6 received the task less than five weeks prior to execution, to plan the communications architecture for IPLC. The USARPAC G39 described the

basic concept to present five keynote speeches and four discussion panels over two days, for four hours per day, with allies and partners in the Pacific theater able to participate through question-and-answer (Q&A). Participants needed to connect from various locations, ranging from Europe to the Indian Ocean, and the audience needed a mechanism to watch in near real-time while submitting written questions and comments for participants to address. The entire content of the conference was intended for public release so confidentiality was not a concern, but availability and integrity were paramount due to the visibility of the conference and its participants (e.g. USINDOPACOM commander, US Army Chief of Staff, etc.).

While the initial requirements involved connecting no more than ten participants at any one time (approximately six geographically distributed panelists, the USARPAC command team, and the production crew), the scope grew to include connecting up to 90 participants simultaneously so that all principals from the 28 invited nations could speak on camera rather than doing only written Q&A.

The final product contained imperfections, but multiple four-star leaders declared the event to be a success that exceeded expectations. Over eight hours of execution, all participants were able to deliver their planned remarks on-schedule with the exception of only one panelist whose connection dropped twice while speaking, forcing the panel moderator to move on with the agenda. All principal outstations that wished to make a comment or ask a question were able to do so. The key elements of the IPLC communications architecture were as follows:

- A Microsoft Teams channel meeting hosted on the ArmyPac Teams tenant for principal participants



Participant from around the world utilized Microsoft Teams to participate in the Indo-Pacific Landpower Conference. Photo provided by Maj. Timothy Walsh

- A Defense Visual Information Distribution Service (DVIDS) live stream
- A Commercial Virtual Remote (CVR) Teams channel for written Q&A and links to the DVIDS live stream for the US DoD audience
- An email inbox to handle written Q&A for non-US DoD audience members watching the DVIDS live stream
- A facility with gigabit-speed commercial Internet service to house the production crew and two conference room systems customized to work with Microsoft Teams

Microsoft Teams was at the heart of the design because of its availability, security assurances, and scale. We had immediate access to both CVR and a separate Teams tenant (ArmyPac) that 311th Theater Signal Command controlled. This availability was in contrast to competing alternatives like WebEx and Zoom for Government which would have taken additional time to acquire. Both CVR and ArmyPac Teams ran in Mi-

crosoft's GovCloud (GCC) which the Department of Defense (DoD) temporarily accredited for up to Impact Level 4 usage with CVR. While confidentiality of For-Official-Use-Only (FOUO) information was not a concern with IPLC, the accreditation did provide some level of assurance about the overall security posture of CVR and ArmyPac Teams, making them better options than the purely-commercial or free, consumer-level alternatives. Finally, while the Defense Information Systems Agency's GVS and DCS platforms were scaled to support thousands of concurrent users, Microsoft Teams was scaled to support tens of millions of concurrent users, leveraging the world's second largest private wide area network peered with hundreds of Internet service providers and giving quality-of-service priority to Teams voice traffic. We judged that IPLC was a "grain of sand in the universe" of Microsoft's Azure cloud platform, such that a failure of Microsoft's platform would be a much bigger story than the failure of IPLC.

One key decision was whether to use the ArmyPac Teams tenant or CVR. Ultimately, we chose to use both for different purposes. We hosted the meeting for principal participants with ArmyPac Teams because we had more control over org-wide meeting settings, guest access and permissions, and audio conferencing licenses. We used CVR Teams for the separate written Q&A channel for US DoD audience members because everyone already had an account, so this required no setup other than giving them a code to join the team.

Microsoft Teams provides built-in functionality for streaming to an audience through its Live Event feature. A Teams Live Event is a type of meeting that draws a clear distinction between who can be on-screen (in the meeting) and who can only watch through a public link on a short delay. The audience may be up to 10,000 people, the audience sees a full screen image of the active speak-



The conference set up inside the Hale Ikena Center on Fort Shafter, Hawaii.

Photo provided by Maj. Timothy Walsh

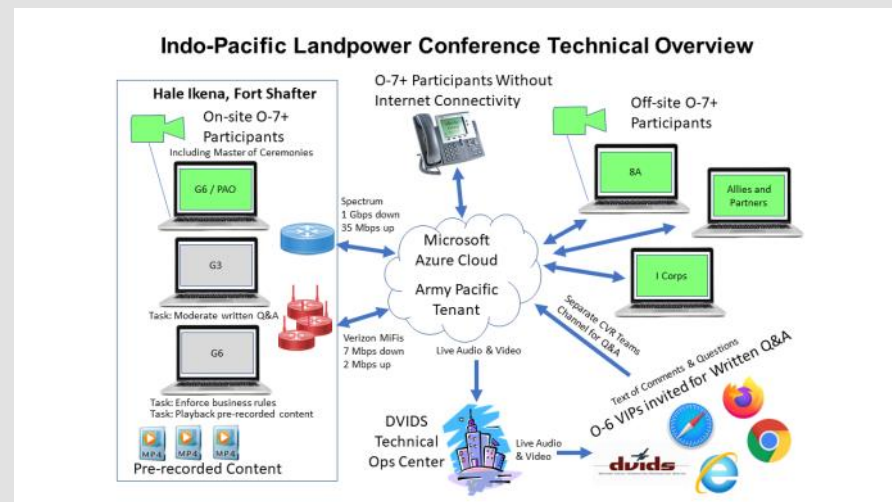
er, and it offers an efficient, native interface for written Q&A. This was initially an important factor in our selection of Microsoft Teams, but we ultimately did not use a Teams Live Event. We found that it worked with only a handful of participants presenting to a larger audience, but beyond that it was buggy. The Teams Meeting format was more appropriate, more familiar, and better tested for the 90 in-meeting participants that we ended up supporting.

To stream a Teams Meeting live to a wider audience, we worked with the Defense Media Activity through USARPAC Public Affairs. We provided login credentials for the Teams Meeting to the Technical Operations Center (TOC) in Atlanta, Georgia, and they used a hardware encoding system to capture the audio and video and embed it on a DVIDS page. Their system could embed a live stream on up to 16 different platforms (Facebook, Twitter, YouTube, etc.) simultaneously, but Public Affairs made a deliberate decision to use only a hidden DVIDS

page for a semi-private audience instead of using USARPAC's public social media accounts. To enable the audience to submit written questions without the built-in Teams Live Event Q&A feature, we created a separate CVR Teams channel that invited audience members could join with a code. While watching the event on DVIDS, audience members posted questions in the CVR Teams channel which the IPLC production crew monitored to copy-and-paste the best questions into the Teams Meeting chat for the master of ceremonies and other participants to handle.

Also at the heart of our design was a Family Morale, Welfare, and Recreation (FMWR) event center on Fort Shafter called the Hale Ikena. At the beginning of the planning process, Microsoft Teams was not yet stable on the Army Pacific network (DoDIN-AP); even 1:1 voice-only sessions were often impossible. In addition, our local Network Enterprise Center (NEC) had not yet approved installation of the Teams desktop application (required for the Live Event feature) nor a variety of other utility programs for audio-video. The performance of Microsoft Teams on DoDIN-AP improved in late April, but we conducted a qualitative survey which found that users still had a 30 percent better experience when using a commercial Internet connection (averaging 4.4 out of 5 stars on commercial Internet vs. 3.3 stars on DoDIN-AP). Therefore, we made an early decision to produce IPLC using standalone computers with commercial Internet service at the Hale Ikena while outstations chose their connection according to their own factors.

We temporarily upgraded the Hale Ikena's commercial Internet service to 1 gigabit-per-second (Gbps) download and 35 megabits-per-second (Mbps) upload bandwidth, and configured a wired local area network (LAN) inside the fa-



Graphic provided by Maj. Timothy Walsh

cility. We aimed for at least 4 Mbps per machine to give ourselves a 2x margin of safety above the official Microsoft recommendation of 2 Mbps for high definition, group video calls, knowing that we would have many machines on-site connected simultaneously.

The production crew used seven laptops (including backups connected to a secondary cellular network) for presenting slides and pre-recorded videos, monitoring participant access and microphones (to mute or remove participants if necessary), and filtering writ-



Graphic provided by Maj. Timothy Walsh

ten Q&A. For on-site panelists and the USARPAC command team, we built two rooms with projectors, speakers, microphone arrays, and 4K cameras on tripods operated by an Armed Forces Network crew.

We used the three doctrinal layers of the cyberspace domain to identify, assess, and mitigate the risks of IPLC. As mentioned earlier, our primary concerns were availability and integrity, not confidentiality.

We judged that our most significant risk in the physical layer, especially with the aging infrastructure on Fort Shafter, was a loss of power and/or Internet connectivity at the Hale Ikena. As a best practice for Live Events, Microsoft recommends having multiple producers with at least one off-site to maintain control during a local failure, and we did something similar.

We had three battery-powered cellular WiFi devices with us in the Hale Ikena, running in parallel with the primary network, and some of the production crew laptops remained connected exclusively to this secondary network. The bandwidth was poor compared to our primary network - just 7 Mbps down and 2 Mbps up - but it was enough to remain connected to the Teams Meeting. We planned to stop sending video if we moved to the secondary network. The master of ceremonies and commanding general also had laptops in front of them connected to the secondary network. They used these laptops primarily for text chat during the event, but they were ready to just put on a headset and continue operations if necessary.

In addition to laptop and WiFi device batteries, we connected our audio-video mixers to uninterruptible power supplies, and we had a small generator on standby to power emergency lighting and other equipment as necessary.

For outstations, we provided the audio conferencing telephone number and conference ID to enable participants to reconnect if they lost Internet service. Microsoft Teams helpfully displays these numbers as a pop-up on the screen when a participant loses connectivity during a meeting. One concern was that we could not authenticate a telephone number before admitting it to the meeting, so we asked participants to first call our separate technical support hotline and give us their phone number, as an extra step, prior to dialing-in. It was also possible to dial a participant's telephone number from the Teams Meeting.

In the logical layer, controlling access was our biggest concern. Again, the issue was not confidentiality, it was limiting access to only invited participants to ensure the availability and integrity of the event. The more people we

had in the meeting, the higher the likelihood that someone would hot-mic or otherwise cause a distraction. In the worst case, without appropriate access controls, an adversary could impersonate a senior leader to disrupt or deface the event. To this end, we disabled anonymous guest access in the organization-wide settings, and we did not distribute a meeting link that an adversary could potentially target. We required all participants to establish a Microsoft Teams account that we could invite to the IPLC Team as a guest member with limited permissions, and we had them join a channel meeting after logging in. In the meeting settings, we set "Who can present?" (able to share desktop, admit people from the lobby, and mute or remove attendees, etc.) to "Only me" and then selected backup presenters ("Make a presenter") from inside the meeting. Here we worked with 311th Theater Signal Command system administrators, the 501st Cyber Protection Team, and Microsoft support representatives to review security settings and ac-

tivity logs for the ArmyPac Teams tenant before and during the event.

Our next biggest concern in the logical layer was a denial-of-service attack against either our LAN or the Microsoft Azure cloud platform hosting our Teams Meeting. We worked with Regional Cyber Center Pacific (RCC-P) to help secure our LAN with a sensor kit to passively monitor for malicious or unusual traffic in real-time. Technicians from 311th and 501st monitored what they could inside of the Microsoft Azure cloud, but we primarily depended on Microsoft's own security posture and the expertise of their site reliability engineers. Again, we judged that a successful denial-of-service attack against the Microsoft Azure cloud would be a much bigger story than the failure of IPLC.

To address one aspect of confidentiality, although the content of IPLC was all publicly releasable, we did not want unauthorized participants to gain access to other FOUO data during IPLC. Using the ArmyPac Teams tenant eliminated this risk because all data on ArmyPac Teams was only Impact Level 2; it did not fall under the temporary DoD waiver to process Impact Level 4 data like CVR Teams.

Finally, we chose to use a fresh, fully up-to-date installation of Windows 10 on all of our standalone laptops, with only the required application software installed to minimize the attack surface. After the event, we wiped the laptops again to ensure removal of credentials and any infection that might have occurred.

Our biggest concerns in the persona layer related to access control: a participant losing their Teams account credentials through phishing or other means, or an adversary dialing-in with a spoofed telephone number. In these cases, our only mitigation was to pay attention and react quickly to remove someone.



Graphic provided by Maj. Timothy Walsh



*The conference set up inside the Hale Ikena Center on Fort Shafter, Hawaii.
Photo provided by Maj. Timothy Walsh*

The most dangerous scenarios would involve an insider threat, which we mitigated through the usual practices of "least privilege" and "separation of privilege" with technicians from multiple entities (311th, 501st, RCC-P, USARPAC G6, etc.) reviewing security settings, activity logs, and network traffic.

Although USARPAC leadership ultimately decided not to host the live stream on public social media platforms, we requested support from the 1st Information Operations Battal-

ion to monitor social media activity for trolling and disinformation so that USARPAC Public Affairs could craft a response, if necessary, to control the strategic narrative.

Finally, for the persona layer, the most likely risk to production quality was having participants who were unfamiliar with the Microsoft Teams interface or their hardware peripherals. Teams was new to our organization, hastily acquired to cope with the pandemic, and none of the principal participants had time for rehearsals given their schedules as senior leaders. We mitigated this as best as possible through one-on-one communications checks with each outstation in the weeks prior to the event, but it was an area in which USARPAC senior leadership had to accept some level of risk. The master of ceremonies explained business rules at the beginning of each session, and during execution it became a best practice for speakers to preface their remarks by asking, "Can everyone hear me OK?" before proceeding.

One lesson learned was that Microsoft Teams proved to be the most stable and capable platform available for large-scale video conferencing at the time, especially on a high-speed commercial Internet connection. Its performance, and the ease of including participants from allied and partner nations, permanently raised the bar for video conferencing in the eyes of USARPAC senior leaders. Our experience was that, on the margin, unlike other DoD systems, adding more users did not cause increased latency or instability or a degradation of audio-video quality. Even participants in nations with poor telecommunications infrastructure, several time-zones away, who tethered their laptop to a mobile phone for connectivity, had a reasonably good experience.

We learned that what did affect performance, on the margin, was the individual network and audio-video setup for each participant. If someone had a bad setup, they generally looked and sounded bad to everyone else, and everyone else looked and sounded bad to them. At the same time, however, everyone else might otherwise have a perfectly good experience. During normal times, when supply chains are not disrupted by a global pandemic, all users should acquire higher-end headsets, 4K USB webcams, digital mixing boards, or all-in-one conferencing devices like the Microsoft Surface Hub for optimal quality.

The biggest production failure we experienced occurred with the DVIDS live stream. The encoding system in the DVIDS TOC crashed during an intermission on the first day. Because it was during intermission, they did not immediately

recognize the problem. By the time our production crew realized the problem, contacted the DVIDS TOC, and got them logged back in, the live stream audience missed approximately 20 minutes of a panel discussion, and DVIDS did not record those 20 minutes at all. To guard against this, we would recommend using a second encoding system and web hosting platform as a backup. We could have encoded the live stream ourselves using a free tool like OBS Studio on a laptop at the Hale Ikena, although we would still need a public-facing web server to host it.



Our most time-consuming challenges and subsequent lessons learned related to access control. As described previously, we chose to create guest accounts for all participants rather than allowing them to connect to the Teams Meeting as external or anonymous users. This had some benefits. It created more of an exclusive, closed environment to which participants had persistent access for communications checks, shared files, and private chats. It allowed us to set proper display names for guests, monitor their activities, and control their permissions at a more granular level so that the 311th and USARPAC commanding generals could be comfortable with the residual risk of extending access to non-US participants. However, creating 90 guest accounts required significant effort, and most of the effort was concentrated in the final days and hours just before execution as the participant list grew exponentially and participants finally made it a priority to follow our instructions to get an account.

In retrospect, we could have made the process easier on everyone by allowing the external and anonymous user access without sacrificing too much security. We would first set "Who can bypass the lobby?" to only "People in my organization." External CVR Teams users must authenticate themselves, so it would be easy for the meeting organizer and other presenters to quickly compare the lobby with a list of invited attendees, and admit people as appropriate (note that this would not work for an event hosted with CVR Teams; all CVR Teams users would be able to bypass the lobby). For non-US participants without a CVR Teams account, we would simply email them a Teams Meeting link and a display name including a unique one-time PIN (e.g. "Major General John Doe, Australian Army, 7716"). As users entered the lobby, we would compare their display name and PIN (7716) with a list of invited attendees, and admit them as appropriate. A one-time PIN prevents a replay attack, so after admitting a participant and crossing them off our list, they would need to call our technical support hotline for a new PIN before re-entering the meeting. Whether we used this method or the method of creating guest accounts, the level of security would ultimately boil down to the trustworthiness of a participant's email inbox.

Ultimately, the success of this event, despite the challenges faced, showed that even once the COVID-19 pandemic wanes, we believe that virtual events will increasingly be part of normal operations in an increasingly connected world, and we offer this contribution to the emerging set of best practices.

Early insights into electronic and cyber warfare at the battalion level

Lt. Col. (ret.) Jose A. Carbone
and Lt. Col. (ret.) John J.
Bastone
Army Futures Command

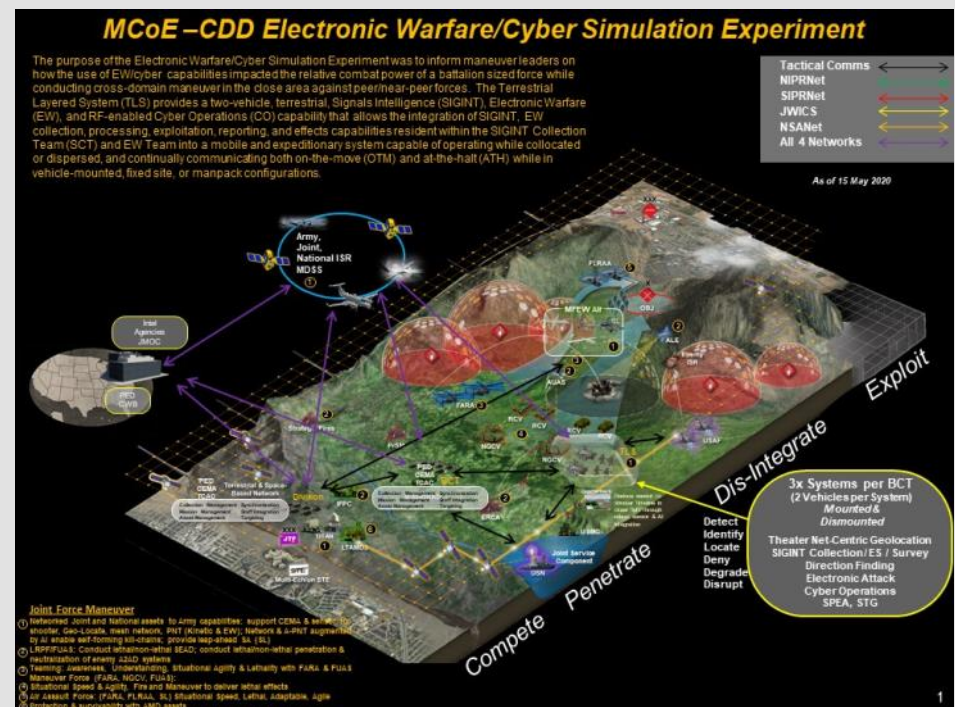
Army Futures Command (AFC) Futures and Concepts Center (FCC) Maneuver Capabilities Development Integration Directorate (MCDID) conducted a constructive simulation experiment (SIMEXp) earlier this year. The SIMEXp's intent was to inform maneuver leaders on the impact of electronic warfare (EW) and cyber capabilities as it related to the relative combat power of a battalion sized force while conducting cross-domain maneuver (CDM) in the close area against peer/near-peer forces. The threat understands the tactical and operational importance of the electromagnetic spectrum (EMS), and have developed and fielded significant electronic warfare (EW) capabilities that directly impact a brigade combat team's (BCT) ability to command and control (C2) forces and synchronize effects. The EMS spans all domains and threat forces place

significant emphasis on EW capabilities, organizing dedicated EW companies, battalions and brigades to ensure control in the EMS. The purpose of the SIMEXp was to inform maneuver leaders how cyber effects integrated with ground and aerial EW capabilities enable Battalion/Squadron sized forces to maneuver to positions of advantage while conducting CDM in support of multi-domain operations (MDO).

The SIMEXp featured a balanced combined arms battalion (CAB) composed of four company teams (2x armor and 2x mechanized) conducting a movement to contact, employing sequentially increased EW and cyber capabilities as it faced a threat motorized rifle company in a hasty defense. The CAB was employed as part of a brigade (notional) augmented with cannon artillery (one battery simulated), and EW support provided by the Terrestrial Layer System (one TLS section simulated). The TLS provides BCTs with an organic multi-disciplined intelligence EW, Cyber, SIGINT capability that bridges the tactical

and operational collection assets used to identify electromagnetic signatures of threat emissions. Threat forces employed proportional organic direct fire weapons, artillery, EW, cyber, and unmanned aircraft systems (UAS) with electronic surveillance (ES) and electronic attack (EA) capabilities.

Tactical Observations of the Terrestrial Layer System (TLS)



Graphic provided by Monica Manganaro

include:

- provided the BCT an ability to access multi-disciplined intelligence electronic warfare, radio frequency enabled cyber, and signal intelligence capability.
- increased situational awareness and understanding and thus informed and increased the speed of tactical decisions and targeting.
- enabled BCTs to better execute command and control and operate semi-independently in a more dispersed manner.
- enabled maneuver formations to conduct semi-independent operations simultaneously maintaining the ability to sense, distinguish, prioritize and target critical threat systems.

BCT's typically rely heavily on organic and supporting aerial and space layer collection assets for tactical intelligence and information. TLS provided the maneuver formation with a bridge between tactical and operational collection assets increasing situational understanding, mitigat-

ing delays in information exchange from National assets, and increasing efficacies of determining courses of actions.

Visualizing and discerning disposition and locations of threat electron-

ic signatures created opportunities for BCTs to influence multiple domains by optimizing the synchronization and sequencing of lethal and non-lethal actions during offensive operations to support CDM and enable MDO.

While it is understood that experimentation is required to better understand employment considerations and the comprehensive impacts associated with integrating the TLS to support cross-domain maneuver, certain insights can be gained as a result of this experiment. Future experimentation should be conducted at the BCT level to ensure all three of the BCT organic TLS, to include the dismounted systems, are incorporated into a future learning event that fully supports the capabilities of the EW/SIGINT/cyber systems and understanding operations in the EMS. This will allow nesting and analytical cross domain integration of functional concepts and capture multilateral successes and challenges by accurately replicating the future operational environment (OE) across all domains, EMS, and information framework.

Respective TRADOC schools must integrate electronic warfare (EW) doctrine, employment practices, and employment considerations into Officer Education System (OES) and Non-Commissioned Officer Education System (NCOES) to increase leader's understanding of EW systems and their ability to



Basis of Issue: 3 Systems (6x vehicles) per BCT

MOS: 4 x 35P (Cryptologic analyst) & 35S (Signals Collection Analyst)
4 x 17E (Electronic Warfare Specialist)

Graphic provided by Monica Manganaro

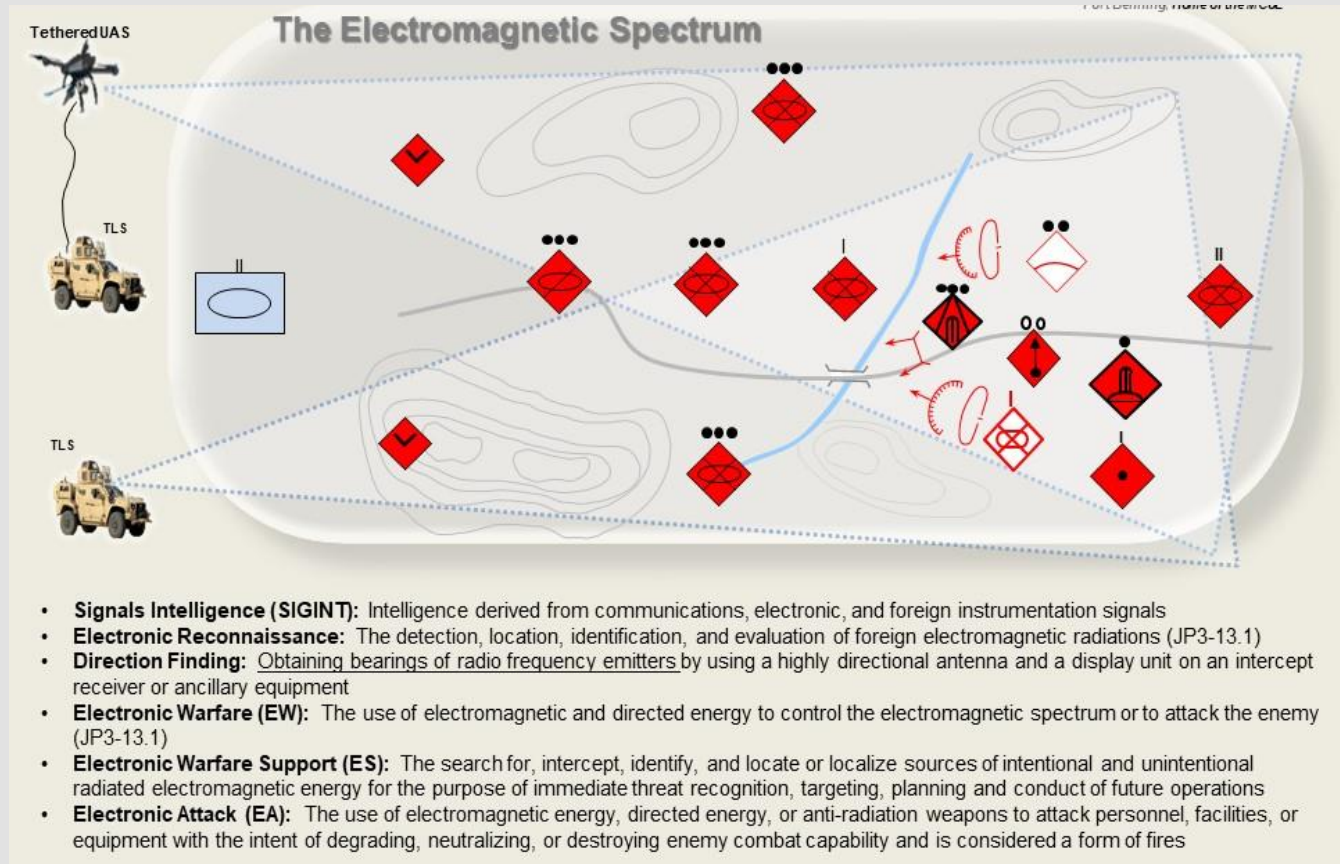
leverage the EMS in support of cross-domain maneuver, in support of multi-domain operations. Respective curricula must address the requirement to plan, coordinate and synchronize EW capabilities/operations with intelligence preparation of the battlefield (IPB), the military decision-making process (MDMP), and rapid decision planning (RDP) to optimize effects and to influence multiple domains. Additionally, EW and Cyber events must be planned into rotations at the combat training centres, in addition to discrete EW and Cyber training venues.

EW and Cyber organizations must be given priority for training and manning. The skill sets required are unique and must be treated as combat multipliers in the event of future conflict. Additionally, opportunities exist for industry to help shape the US Army's proficiency in EW and Cyber through the creation of advanced modeling and simulation technology in order to incorporate the use of Artificial Intelligence (AI). Using AI will assist in decreasing the time it

takes to reduce, analyze and interpret data therefore increasing the units operational tempo. This will enable the Army to test, validate, and improve concepts for future force designs in support of multi-domain operations.

The threat currently is employing and will employ EW and cyber effects across the spectrum of conflict. It is incumbent on US forces to have the capability to successfully mitigate those effects. This experiment demonstrated the potential of organic EW and cyber capabilities at the BCT level.

Authors' Note: the information in this article was extracted from MCDID Maneuver Battle Laboratory Final Report, Maneuver Battle Lab Project 442, CDD SIMEXp, January 6 – 24, 2020.



Graphic provided by Monica Manganaro

2020 AFCEA ARMY SIGNAL CONFERENCE

JULY 14-16, 2020 • ONLINE AND ON-DEMAND!

DATA: "THE AMMUNITION OF THE FUTURE FIGHT"

SPONSORED BY AFCEA INTERNATIONAL



During 2019, the U.S. Army continued to modernize networks and integrate new technology and solution providers – all to meet the requirements of the national defense strategy, threat realities, and multi-domain operations. The speed of change increases. Enabling this change are key enterprise level decisions by DoD and all Services related to technology advances, cloud services, and both data design and management. Central concerns remain regarding talent management, training, and delivery of services.

To address these important topics, the Army CIO leadership and supporting industry will gather virtually July 14-16 at the AFCEA Army Signal Conference to address the theme, **Data: "The Ammunition of the Future Fight."** Participants will focus on the issues, the opportunities, the initiatives, and the solutions related to this key component in the design of future command, control and communications supporting our Army.

For more information or to register to participate, please visit www.afcea.org/event/ArmySignalConference.

In the next



ARMY



COMMUNICATOR

**Through
the eyes of
Combat
Camera**

